



FIG. 1

2/3

20

INITIAL SOFTWARE PRODUCT ~21

MANUFACTURER:

GENERATE ENCRYPTION KEY A ~22

GENERATE ONE OF EITHER SPLIT A OR TOKEN ~24

CALCULATE OTHER OF SPLIT A OR
TOKEN USING KEY A SUCH THAT
SPLIT A + TOKEN = KEY A:
 $\therefore \text{SPLIT A} = \text{KEY A} \oplus \text{TOKEN}$ ~25

ENCRYPT INITIAL SOFTWARE
PRODUCT WITH KEY A ~26

INSTALL INITIAL SOFTWARE PRODUCT
AND SPLIT A IN HARDWARE PRODUCT ~28

DELIVER TOKEN AND
HARDWARE PRODUCT TO CUSTOMER ~29

CUSTOMER:

INSERTS TOKEN ~30

HARDWARE PRODUCT COMBINES TOKEN
 \oplus SPLIT A TO PROVIDE KEY A ~32

HARDWARE PRODUCT USES KEY A
TO DECRYPT INITIAL SOFTWARE ~34

FIG. 2

3/3

40

DIFFERENT VERSION
OF SOFTWARE PRODUCT ~39

MANUFACTURER:

GENERATE ENCRYPTION **KEY B**

~42

ENCRYPT DIFFERENT VERSION OF
SOFTWARE PRODUCT WITH **KEY B**

~43

GENERATE UPDATE
SPLIT = KEY A \oplus KEY B

~44

PROVIDE DIFFERENT VERSION OF
SOFTWARE PRODUCT AND **UPDATE**
SPLIT TO CUSTOMER

~45

CUSTOMER:

INSTALL ENCRYPTED DIFFERENT
VERSION OF SOFTWARE PRODUCT
AND **UPDATE SPLIT**

~46

COMBINE UPDATE SPLIT AND
SPLIT A TO GENERATE
SPLIT B = TOKEN \oplus KEY B

~47

INSERT TOKEN

~48

COMBINE TOKEN AND
SPLIT B TO PROVIDE **KEY B**

~49

USE **KEY B** TO DECRYPT DIFFERENT
VERSION OF SOFTWARE PRODUCT

~50

FIG. 3